Internet Explorer Security

Rob Franco
Lead Program Manager
Microsoft Corporation

Overview

- Background on Web Browser Vulnerabilities
- Designed for security
  - Security updates for existing products
  - Security enhancements for IE in XP SP2
  - Security enhancements for trustworthy browsing in Longhorn

Browser Vulnerabilities

- All Web Clients face similar vulnerabilities
  - Cross Domain
  - Malicious Downloads
  - Spoofing
  - Vulnerable extensibility (eg. ActiveX or Plug-in)
  - Buffer Overruns

demo

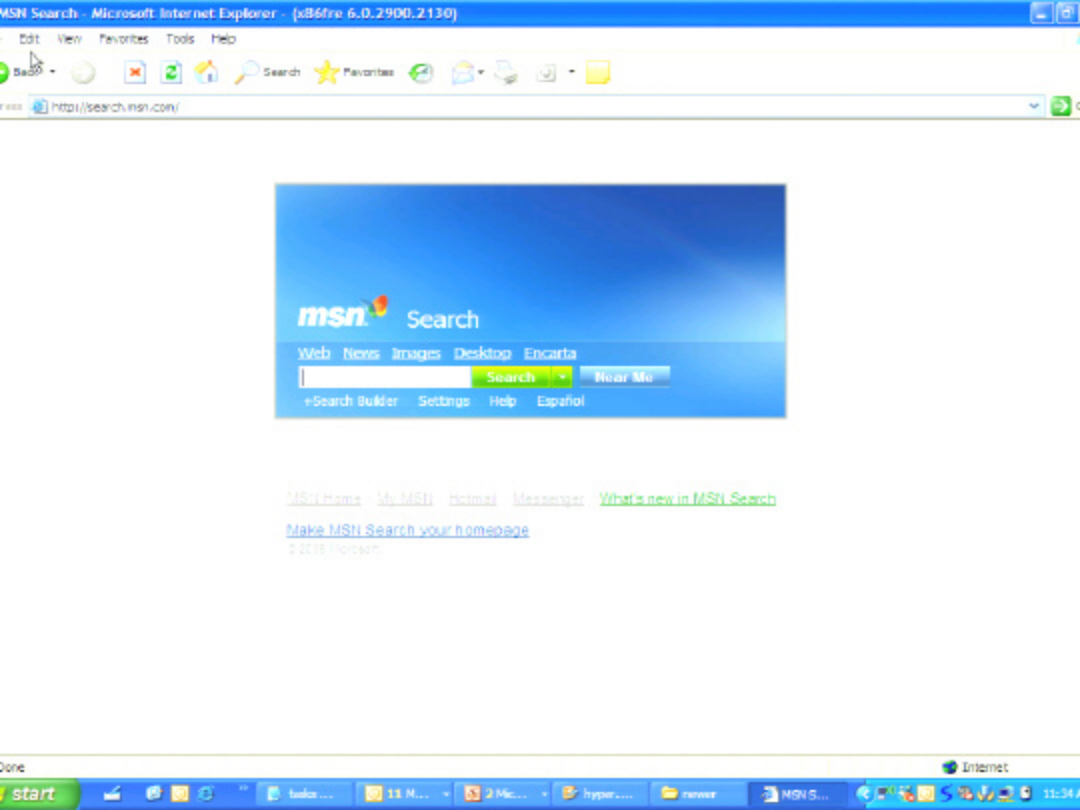
UI Spoofing with of a fullscreen window

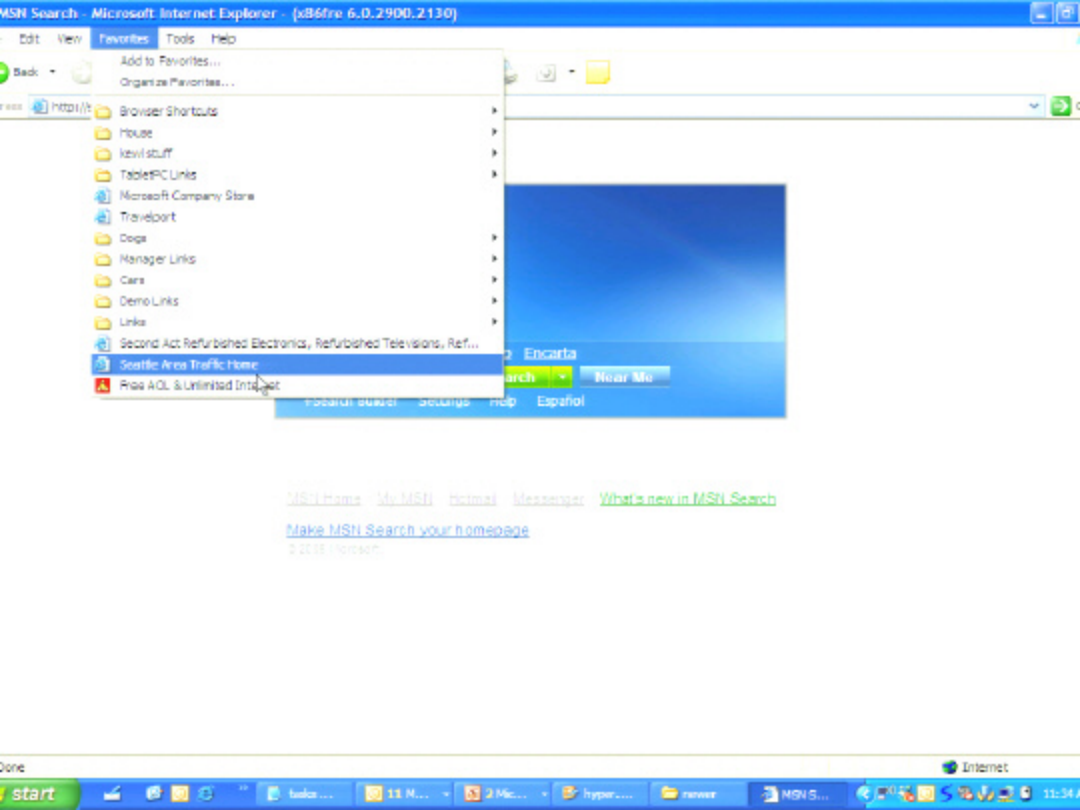
demo

UI Spoofing with of a fullscreen window

demo

UI Spo of a fullscreen window

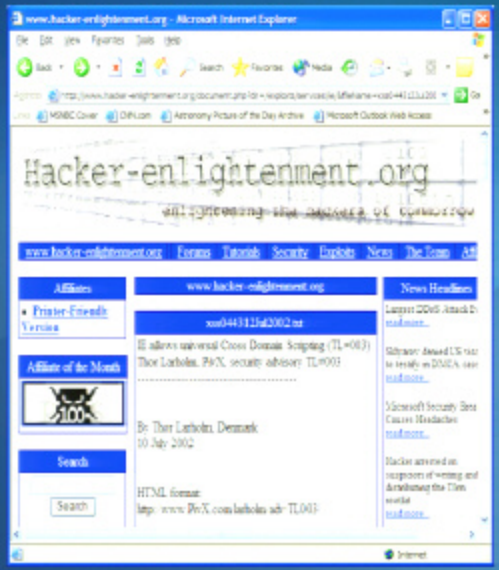

MSN Search - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Search
Favorites
http://search.msn.com/
msn Search
Web News Images Desktop Encarta
Search
Near Me
+Search Builder Settings Help Español
MSN Home My MSN Hotmail Messenger What's new in MSN Search
Make MSN Search your homepage
Done
Internet
start


MSN Search - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Add to Favorites...
Organize Favorites...
Browser Shortcuts
House
kewl stuff
TabletPC Links
Microsoft Company Store
Travelport
Dogs
Manager Links
Cars
Demo Links
Links
Second Act Refurbished Electronics, Refurbished Televisions, Ref...
Seattle Area Traffic Home
Free AOL & Unlimited Internet
Encarta
Near Me
Español
MSN Home
My MSN
Hotmail
Messenger
What's new in MSN Search
Make MSN Search your homepage
Done
Internet
start

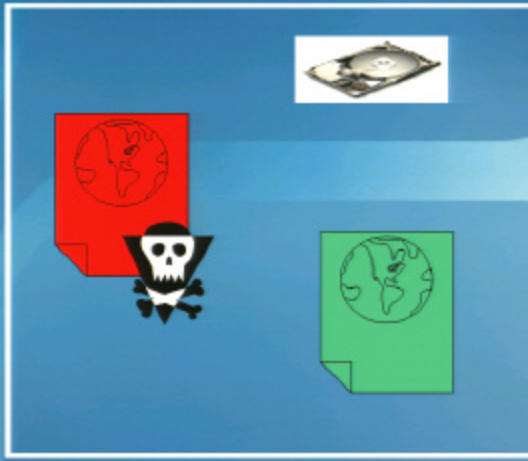
is is Full screen

ot

Browser Vulnerabilities
Cross Domain



- Can affect any client software
- Allows the attacker to inject or steal data from another domain on the user's behalf



Browser Vulnerabilities

Cross Domain

Mobile code has to go through a domain check in order to access the element.

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	GREEN
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.abc.com

Browser Vulnerabilities

Cross Domain

Mobile code has to go through a domain check in order to access the element.

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	GREEN
Size	32
Text	Important Data
[redacted]	
Domain	ww

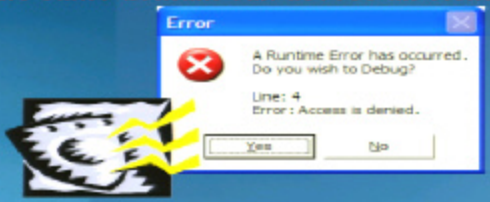
Important Data

Script	MyH.color="RED"
[redacted]	
Domain	www.abc.com

Cross Domain Security

RULE #1 : Only Script from the same domain can access an element

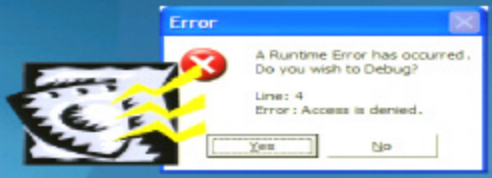
Element	<H>
ID	MyH
Color	Green
Size	32
Text	Important Data
Domain	www.abc.com



Cross Domain Security

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	Green
Size	32
Text	Important Data
Domain	www.abc.com



Cross Domain Security

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	Green
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.evil.com

Browser Vulnerabilities

Cross Domain

Mobile code has to go through a domain check in order to access the element.

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	GREEN
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.abc.com

Cross Domain Security

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	Green
Size	32
Text	Important Data
Domain	www.abc.com

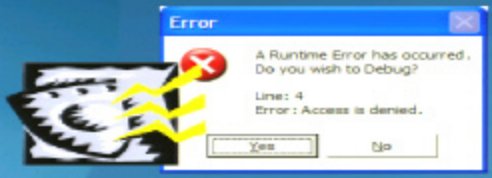
Important Data

Script	MyH.color="RED"
Domain	www.evil.com

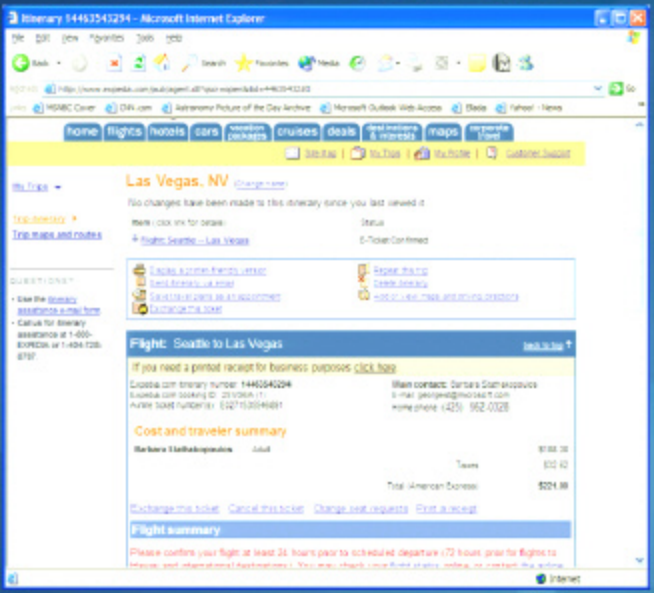
Cross Domain Security

RULE #1 : Only Script from the same domain can access an element

Element	<H>
ID	MyH
Color	Green
Size	32
Text	Important Data
Domain	www.abc.com

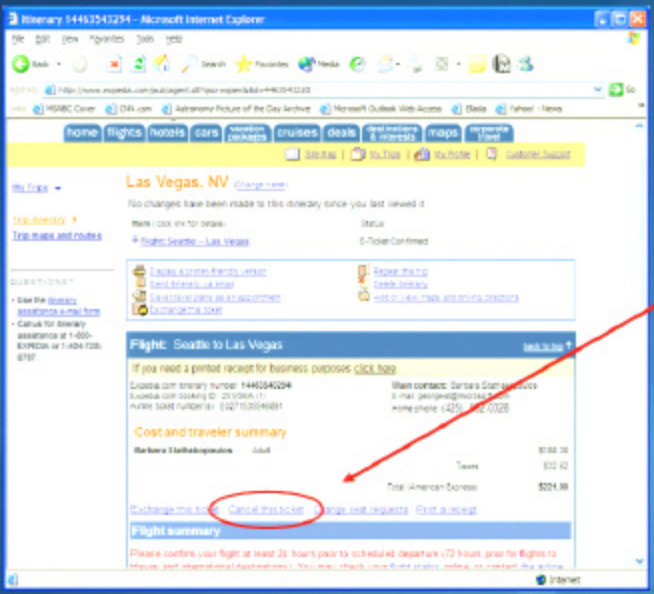


Cross Domain Security Exploits




```
<A> ID=A2003_19834
    HREF="/pub/agent.dll?qscr=cncl&itid=44635432&itdx=0&acmd=aflt&vwtp=2">
    Cancel this ticket
</A>
```

Cross Domain Security Exploits



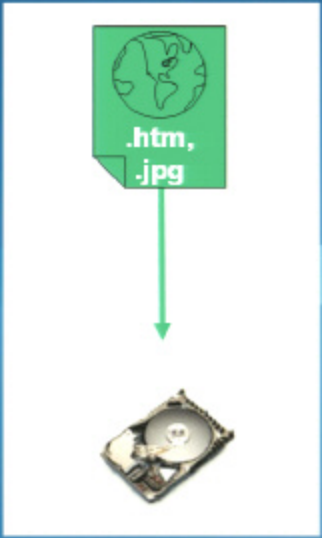

```
x=window.open("www.expedia.com");
x.item(A2003_19834).navigate;
```

```
<A> ID=A2003_19834
    HREF="/pub/agent.dll?qscr=cncl&itid=44635432&itdx=0&acmd=aflt&vwtp=2">
    Cancel this ticket
</A>
```

Browser Vulnerabilities
Malicious downloads

Web browsers should not automatically download dangerous file types like .exe, .bat, .cmd or .hta

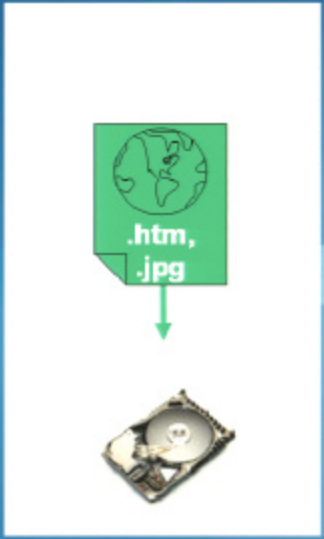
- However…
  - Web servers may provide bogus file type information designed to trick file download logic
  - Web servers may encode the file name to hide a dangerous file extension
- .. and sometimes users are just nagged into downloading a malicious exe



Browser Vulnerabilities
Malicious downloads

Web browsers should not automatically download dangerous file types like .exe, .bat, .cmd or .hta

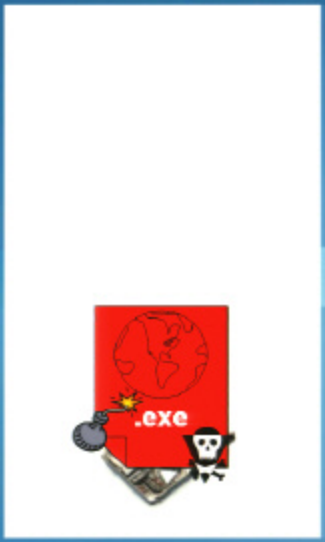
- However…
  - Web servers may provide bogus file type information designed to trick file download logic
  - Web servers may encode the file name to hide a dangerous file extension
- .. and sometimes users are just nagged into downloading a malicious exe



Browser Vulnerabilities
Malicious downloads

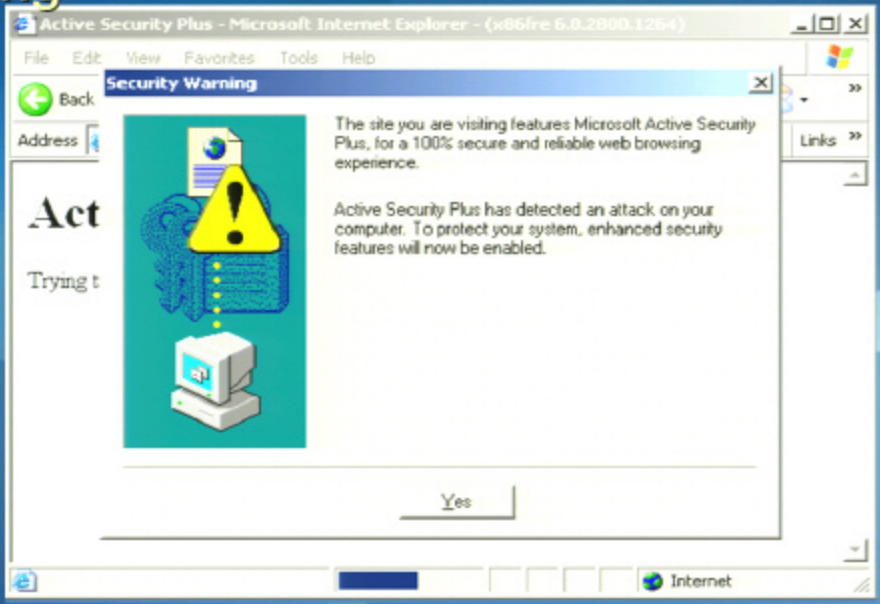
Web browsers should not automatically download dangerous file types like .exe, .bat, .cmd or .hta

- However…
  - Web servers may provide bogus file type information designed to trick file download logic
  - Web servers may encode the file name to hide a dangerous file extension
- .. and sometimes users are just nagged into downloading a malicious exe

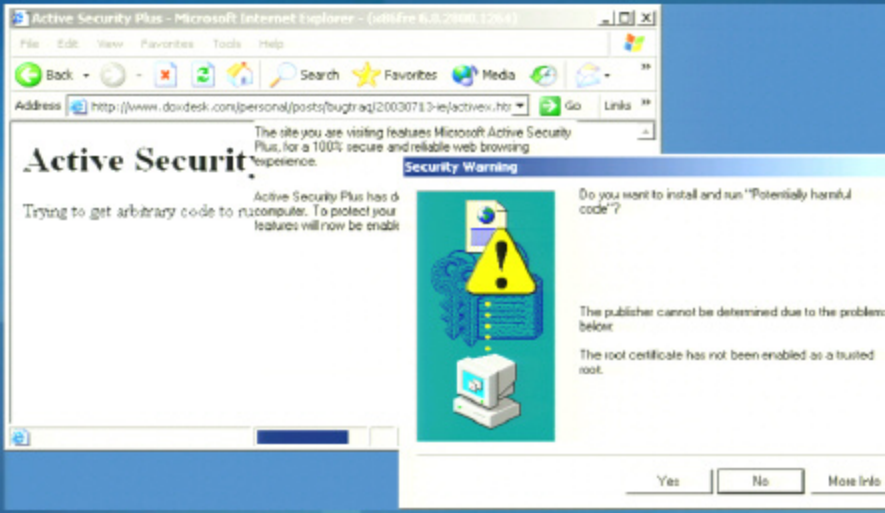


Browser Vulnerabilities

Spoofing

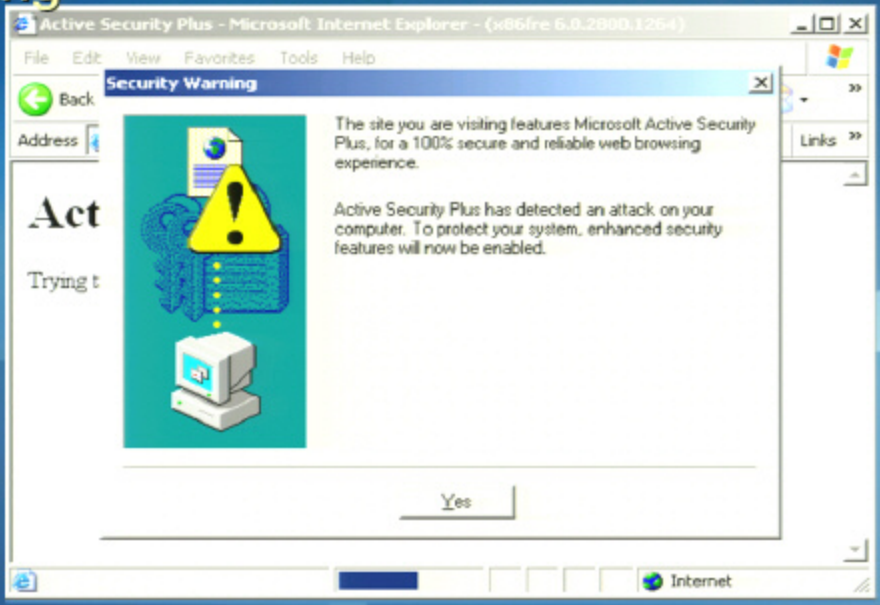


Browser Vulnerabilities
Spoofing

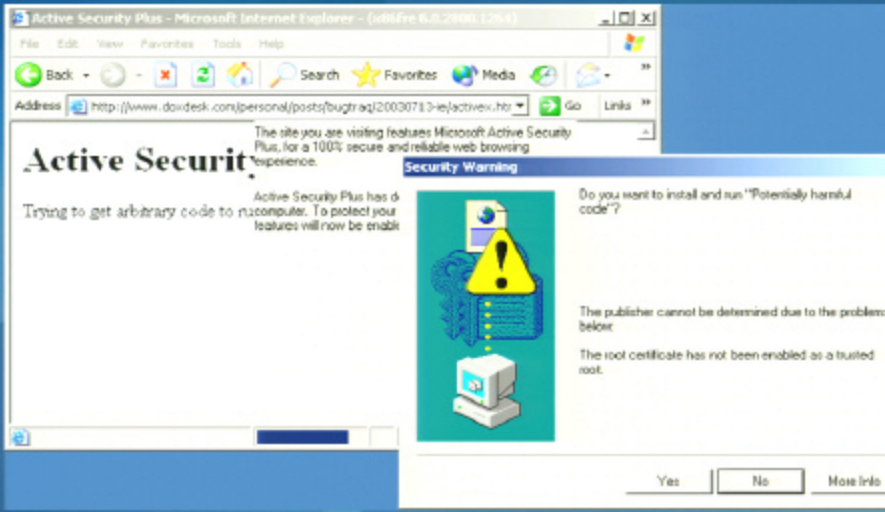


Browser Vulnerabilities

Spoofing



Browser Vulnerabilities
Spoofing



Browser Vulnerabilities

Vulnerable ActiveX/extensibility

- Developers writing binary extensibility have to implement their own
  - Cross Domain Security
  - Cross Site Scripting Security
  - Buffer Overrun Protection
- Developers can make their controls SFI/SFS and sign them but they have to implement their own security when the controls expose dangerous functions
- A dangerous function usually enables functionality that circumvents the Browsers security
- If a control exposed dangerous function it must protect against use by an evil site

Dangerous Functions
Access the File System
Access a device such as • microphones • modems • printers
Launch Programs
Change Security Settings
Write in Registry
Shutting down the system
Accessing Address books
Access Browsing history
Installing Files
Logging users
Enable File Transfer

Browser Vulnerabilities

Buffer Overruns

Element	<IMG>
SRC	..\BufferOverrun.jpg
Domain	www.evil.com


```
<H1>
<IMG SRC = "xxx...xxxx">
  George
</H1>
```

```
szImagePath[20];
lstrcpy(szImagePath, szUserInput);
```

Goal:

Find a place where the parser does not check for size of an argument

Browser Vulnerabilities

Buffer Overruns

Element	<IMG>
SRC	..\BufferOverrun.jpg
Domain	www.evil.com


```
<H1>
<IMG SRC = "xxx…xxxx">
  George
</H1>
```

```
szImagePath[20];
lstrcpy(szImagePath,"xxx…xxxx");
```

Goal:

Find a place where the parser does not check for size of an argument

Designed for Security

- Security investments are driven by customer benefit
  - Security Updates address known issues and ship through Windows Update
    - Fixes are targeted at specific vulnerabilities to preserve AppCompat
    - Customer hotfix binaries are also updated with the same security fixes
  - Major releases include aggressive security improvements
    - Enhanced security rules mitigate entire classes of attacks
    - End-user features educate and provide more control over security decisions
    - Compat workarounds are where-ever possible to ease deployment
- ***All*** changes go through threat modeling, penetration testing and code analysis tools

Designed for Security
IE for XP SP2

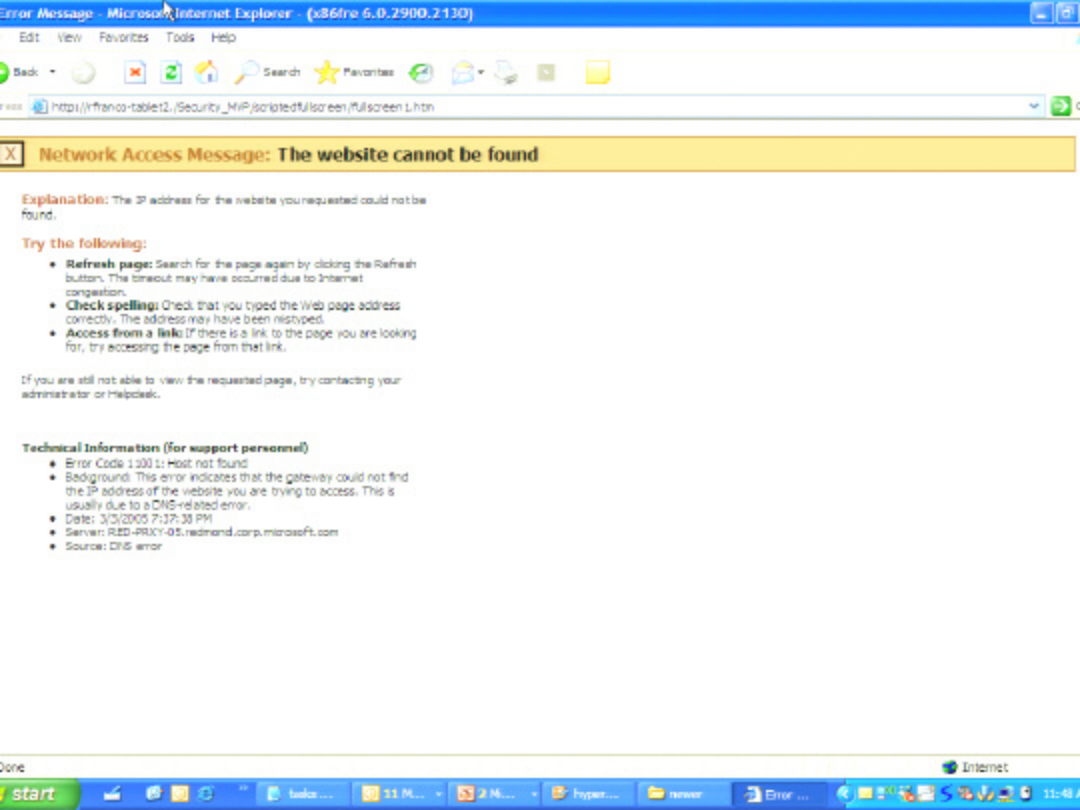
- With IE for XP SP2 you can
  - Browse anywhere and have a safer Internet experience
  - Avoid unwanted pop-up windows and downloads
  - Continue to use your existing applications and favorite websites with few problems

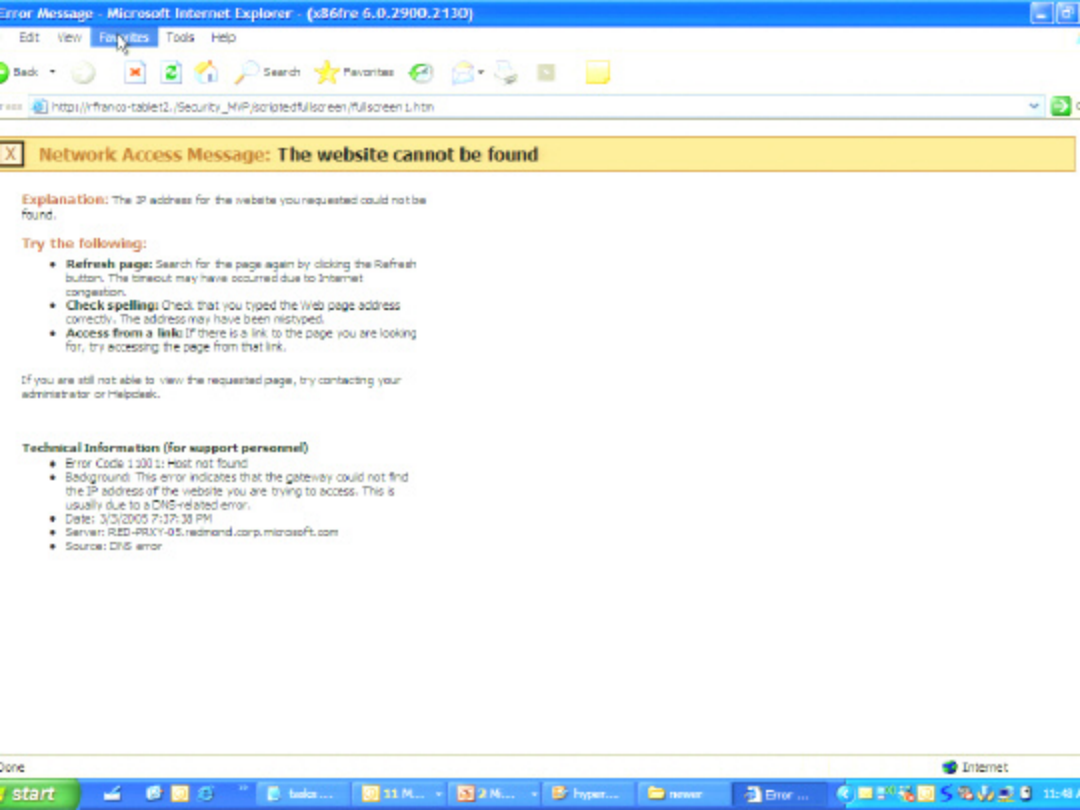
demo

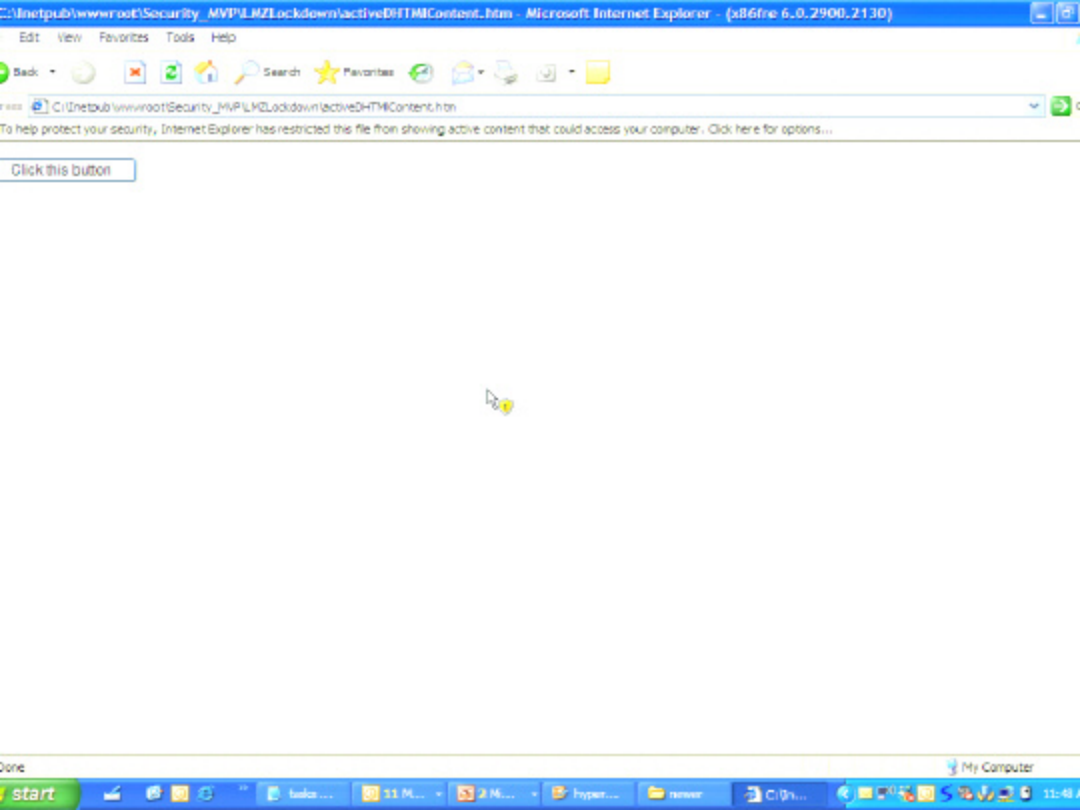
Local Machine Zone Lockdown

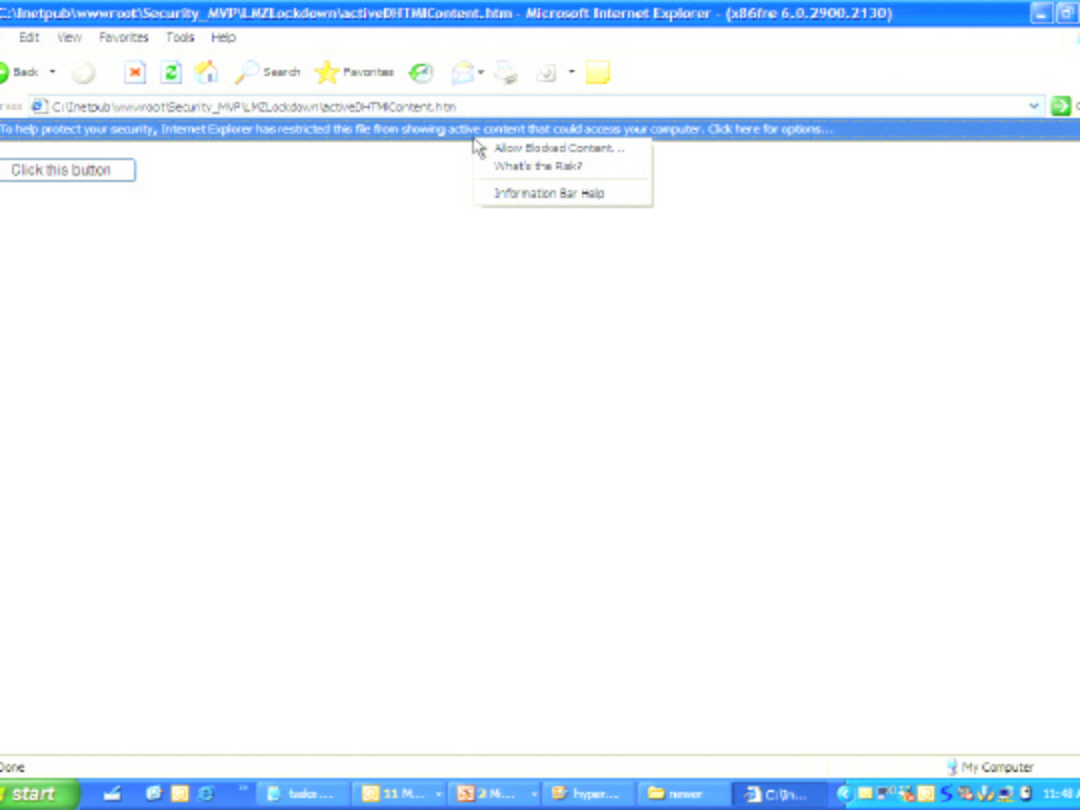
demo

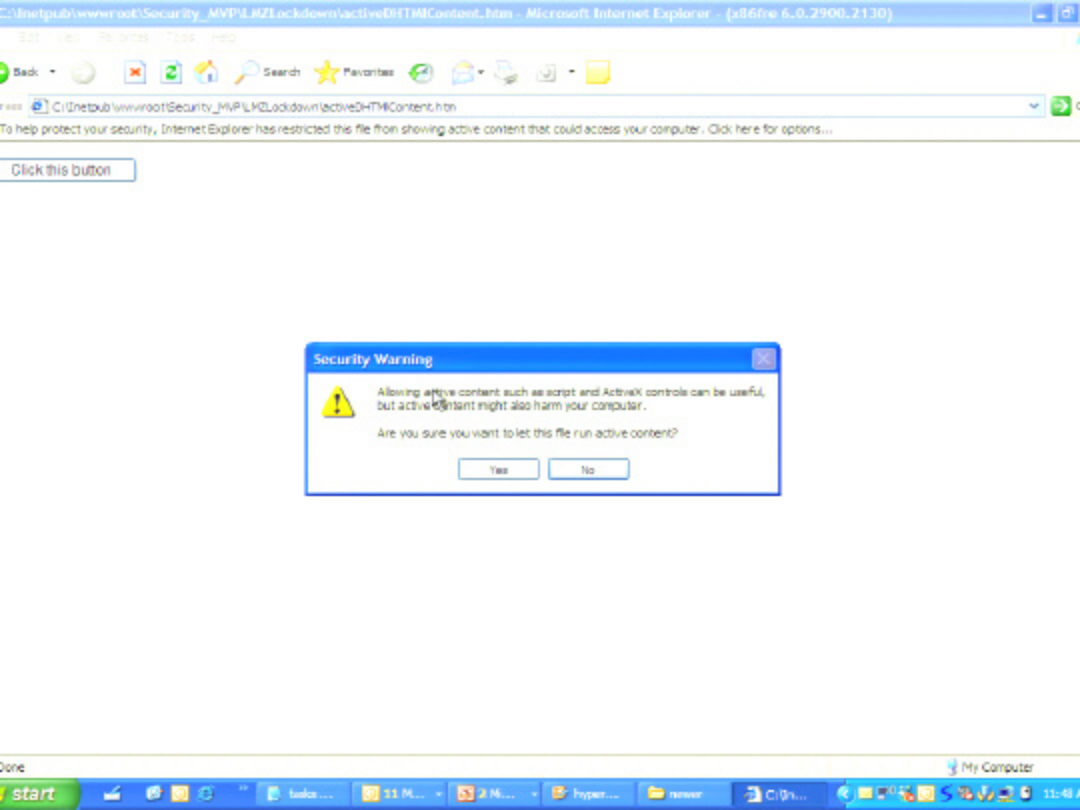
Local Machine Zone Lockdown

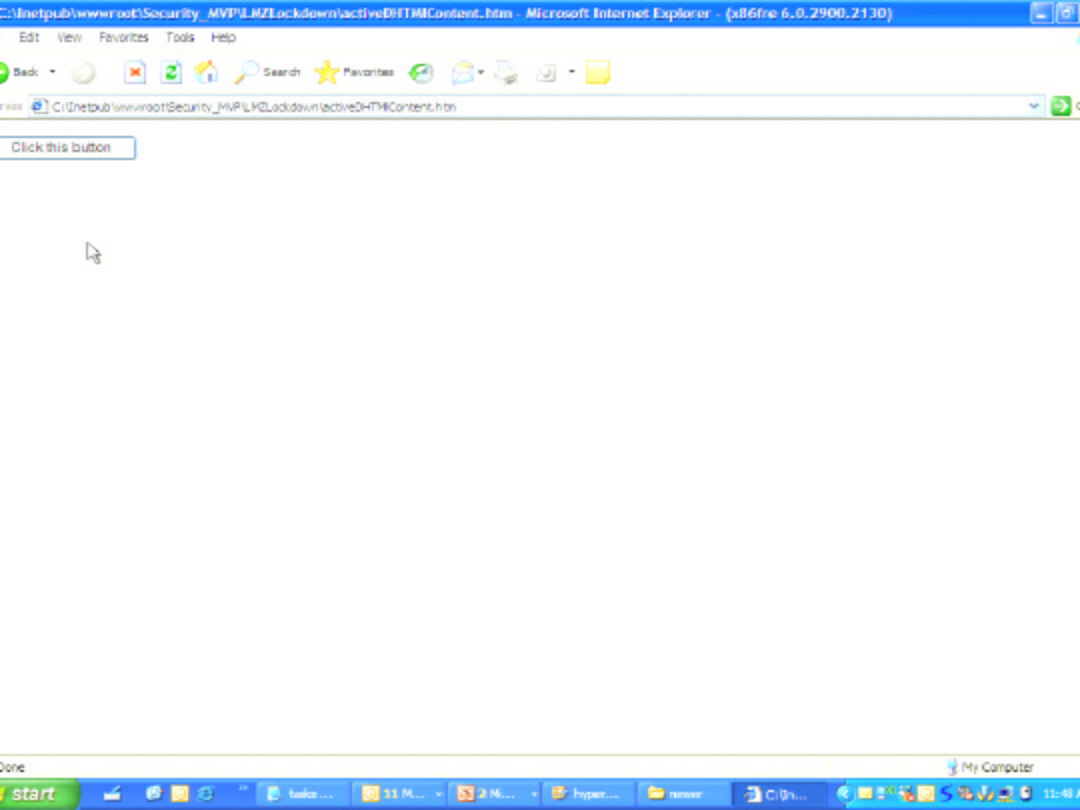

Error Message - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Back Search Favorites
http://franco-tablet2./Security_MVP/scriptedfullscreen/fullscreen1.htm
Network Access Message: The website cannot be found
Explanation: The IP address for the website you requested could not be found.
Try the following:
Refresh page: Search for the page again by clicking the Refresh button. The timeout may have occurred due to Internet congestion.
Check spelling: Check that you typed the Web page address correctly. The address may have been mistyped.
Access from a link: If there is a link to the page you are looking for, try accessing the page from that link.
If you are still not able to view the requested page, try contacting your administrator or Helpdesk.
Technical Information (for support personnel)
Error Code 1100 1: Host not found
Background: This error indicates that the gateway could not find the IP address of the website you are trying to access. This is usually due to a DNS-related error.
Date: 3/3/2005 7:17:38 PM
Server: RED-PROXY-05.redmond.corp.microsoft.com
Source: DNS error
Done
Internet
start


Error Message - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Back Search Favorites
http://franco-tablet2./Security_MVP/scripted/fullscreen/fullscreen1.htm
X
Network Access Message: The website cannot be found
Explanation: The IP address for the website you requested could not be found.
Try the following:
Refresh page: Search for the page again by clicking the Refresh button. The timeout may have occurred due to Internet congestion.
Check spelling: Check that you typed the Web page address correctly. The address may have been mistyped.
Access from a link: If there is a link to the page you are looking for, try accessing the page from that link.
If you are still not able to view the requested page, try contacting your administrator or Helpdesk.
Technical Information (for support personnel)
Error Code 11001: Host not found
Background: This error indicates that the gateway could not find the IP address of the website you are trying to access. This is usually due to a DNS-related error.
Date: 3/3/2005 7:17:38 PM
Server: RED-PRXY-05.redmond.corp.microsoft.com
Source: DNS error
Done
Internet
start
Error ...
11:48


C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Back
Search
Favorites
C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
Click this button
Done
My Computer
start


C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMlContent.htm - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Back
Search
Favorites
C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMlContent.htm
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
Allow Blocked Content...
What's the Risk?
Information Bar Help
Click this button
Done
My Computer
start


C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Back
Search
Favorites
C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
Click this button
Security Warning
Allowing active content such as script and ActiveX controls can be useful, but active content might also harm your computer.
Are you sure you want to let this file run active content?
Yes
No
Done
My Computer
start

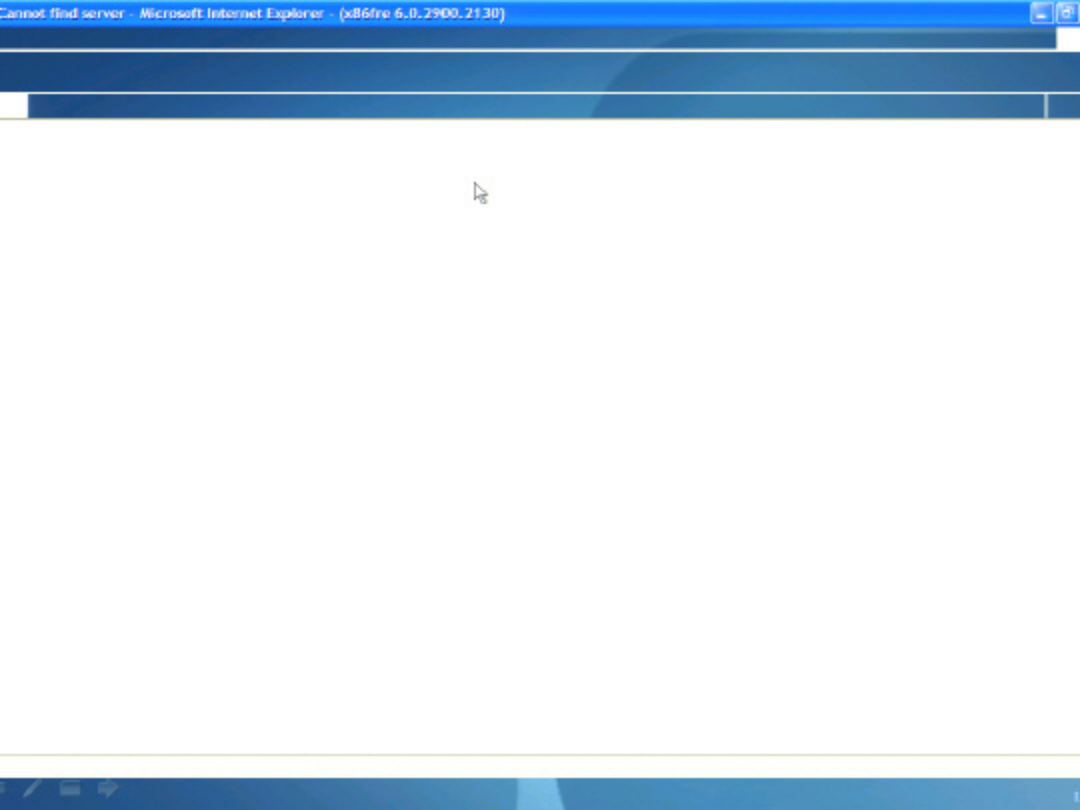

C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)
Edit View Favorites Tools Help
Back
Search
Favorites
C:\Inetpub\wwwroot\Security_MVP\LMZLockdown\activeDHTMLContent.htm
Click this button
Done
My Computer
start

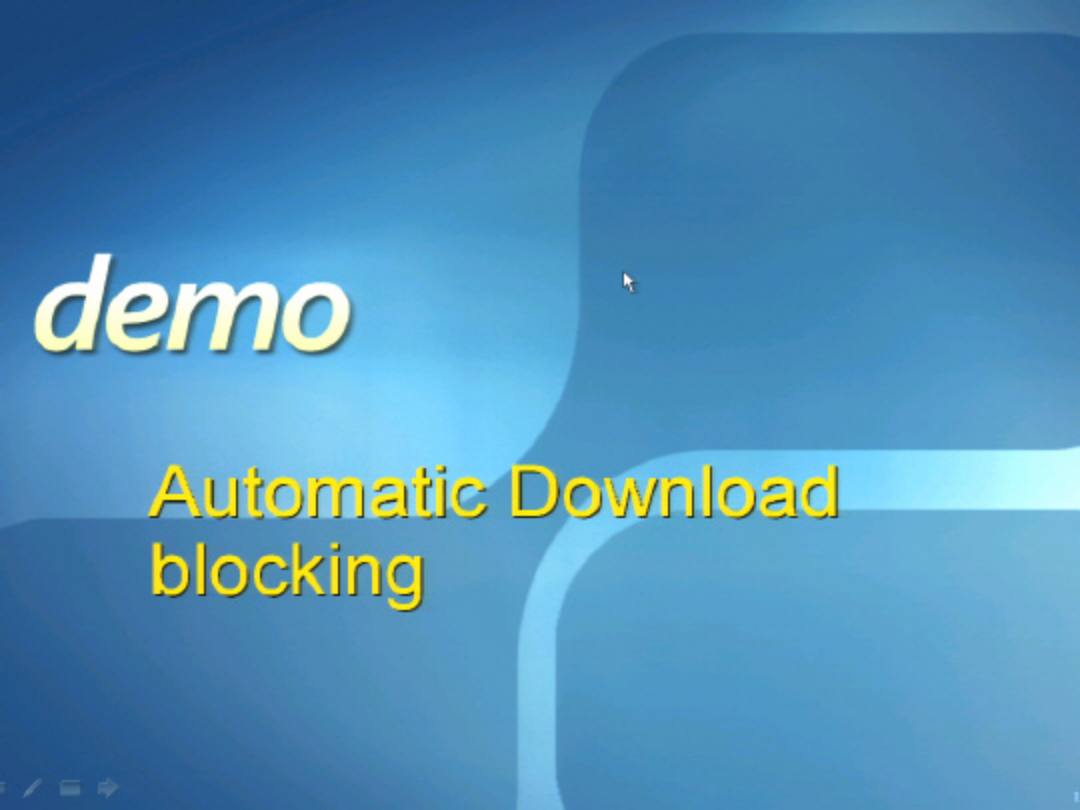
Designed for Security
IE for XP SP2

- More protection against **Spoofing**
  - Restricts scripted windows in the internet zone
- More protection against **Vulnerable ActiveX/ Extensibility**
  - Blocks automatic downloads of ActiveX controls
  - ActiveX Ctrls and BHOs can be managed with the Manage Add-ons control panel
  - Blocks the download of test-signed ActiveX
  - Blocks the use of Binary Behaviors in email scenarios
  - Fewer ActiveX controls are included in Windows by default
- More protection against **Buffer Overruns** through automated code improvements

demo

Automatic Download blocking


Cannot find server - Microsoft Internet Explorer - (x86fre 6.0.2900.2130)


demo
Automatic Download
blocking

Lessons Learned from SP2

- Customers need Security *and* Compat
  - Beta feedback tunes the balance
  - All mitigations are designed for IE first and opt-in for other apps that host IE
  - Compat workarounds must be simple and effective
- Vulns found since SP2 have us treating historic vulns as if they are living threats
  - ActiveX controls expand the attack surface
  - Drag and Drop
- Further response needed against emerging threats
  - Spyware downloads through vulnerabilities
  - Phishing sites that spoof users to give up personal info

Lessons Learned from SP2

- Customers need Security *and* Compat
  - Beta feedback tunes the balance
  - All mitigations are designed for IE first and opt-in for other apps that host IE
  - Compat workarounds must be simple and effective
- Vulns found since SP2 have us treating historic vulns as if they are living threats
  - ActiveX controls expand the attack surface
  - Drag and Drop
- Further response needed against emerging threats
  - Spyware downloads through vulnerabilities
  - Phishing sites that spoof users to give up personal info

Designed for Security
IE for Longhorn

- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened URL Parsing logic
  - IE may run with lower privilege
- More secure defaults for extensibility
  - Info Bar for pre-installed ActiveX
  - Safe-boot IE runs with no addons
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location

Designed for Security
IE for Longhorn

- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened URL Parsing logic
  - IE may run with lower privilege
- More secure defaults for extensibility
  - Info Bar for pre-installed ActiveX
  - Safe-boot IE runs with no addons
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location

Designed for Security
IE for Longhorn

- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened URL Parsing logic
  - IE may run with lower privilege
- More secure defaults for extensibility
  - Info Bar for pre-installed ActiveX
  - Safe-boot IE runs with no addons
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location

Designed for Security
IE for Longhorn

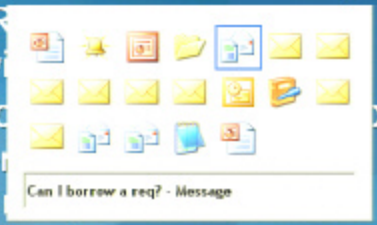
- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened UR
  - IE may run wi
- More secure c ility
  - Info Bar for pr
  - Safe-boot IE
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location

Designed for Security
IE for Longhorn

- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened URL Parsing logic
  - IE may run with lower privilege
- More secure defaults for extensibility
  - Info Bar for pre-installed ActiveX
  - Safe-boot IE runs with no addons
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location

Designed for Security
IE for Longhorn

- Architecture changes
  - Hardened Cross Domain boundary
  - Hardened UR
  - IE may run wi
- More secure c ility
  - Info Bar for pr
  - Safe-boot IE
- Anti-phishing features
  - Fraud-retardant address bar and SSL indicators
  - Anti-phishing service to protect users from known phishing URLs
- Keep your browsing information private
  - Clear your browsing history in one location



Untitled Message

File Edit View Insert Format Tools Table Window Help

Type a question for help

Normal + Arial, Arial 10 B I U

Send Accounts Options... Rich Text

To... Kotov, Erik

Cc...

Subject:

crosoft, is the world leader in personal computer operating systems and productivity software.

esire to expand career options and build skills for larger role

lic servant

crosoft is the world leader in personal computer operating s

ftware Test Engineer, Microsoft Office

Programmed and tested features to allow unattended

ka "Systems Management Server 2.0"

Drafted user guide for my features

Designed and hosted a customer workshop at the A

anted to lead more of the design process and the strategic

position on the Internet Explorer product team

s Metal Fabricating division creates stamped and milled auto parts for General Motors Assembly plants

esigned and programmed an application for project managers to report resource allocations into a central database that was used to project the plant's operating budget quirements.

ernship ended, accepted a full time job with Microsoft after graduation.

o Franco

n to change the world tomorrow? Join the new IE team today

start

Microsoft PowerPoint - [TCAAB IE Security Presentation.ppt]

Microsoft PowerPoint - [TCAAB IE Security Presentation.ppt]

File Edit View Insert Format Tools Slide Show Window Help

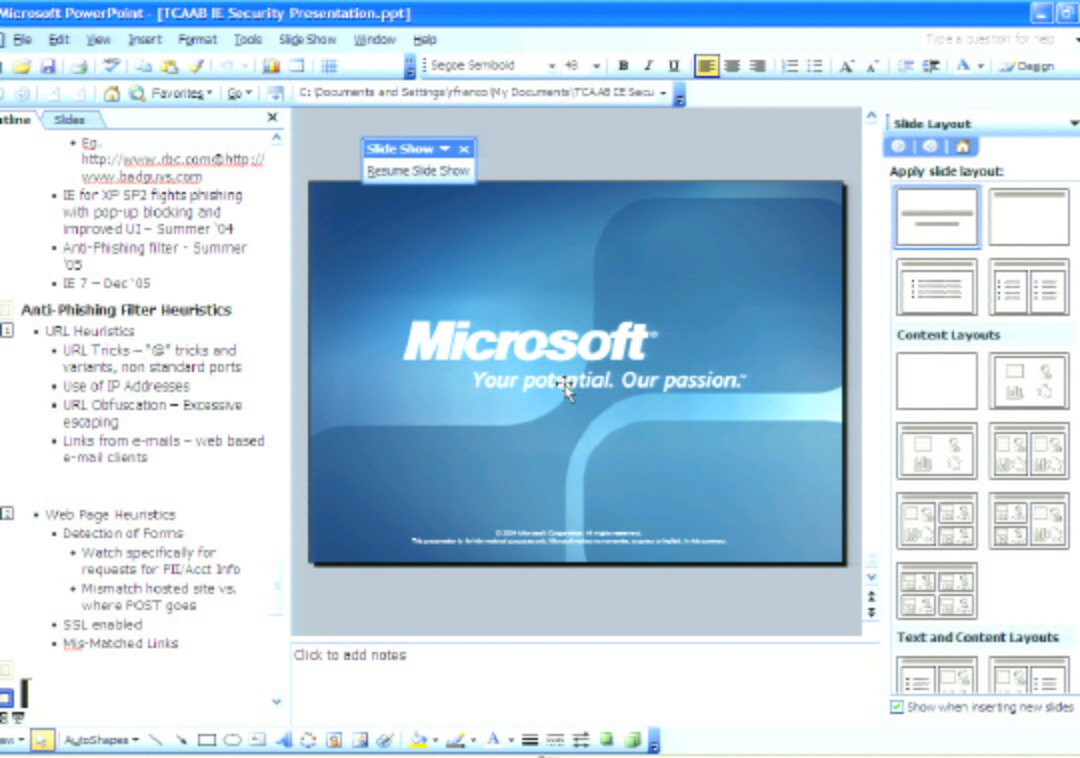
Type a question for help

Segoe Semibold 48 Design

Favorites Go C:\Documents and Settings\franco\My Documents\TCAAB IE Secu

Slide Layout

AutoShapes


Microsoft PowerPoint - [TCAAB IE Security Presentation.ppt]
File Edit View Insert Format Tools Slide Show Window Help
Favorites Go
C:\Documents and Settings\yfranco\My Documents\TCAAB IE Secu
Slides
• Eg. http://www.rbc.com@http://www.badguys.com
• IE for XP SP2 fights phishing with pop-up blocking and improved UI – Summer '04
• Anti-Phishing filter - Summer '05
• IE 7 – Dec '05
Anti-Phishing Filter Heuristics
• URL Heuristics
• URL Tricks – "@" tricks and variants, non standard ports
• Use of IP Addresses
• URL Obfuscation – Excessive escaping
• Links from e-mails – web based e-mail clients
• Web Page Heuristics
• Detection of Forms
• Watch specifically for requests for PII/Acct Info
• Mismatch hosted site vs. where POST goes
• SSL enabled
• Mis-Matched Links
Slide Show
Resume Slide Show
Microsoft
Your potential. Our passion.
Click to add notes
Slide Layout
Apply slide layout:
Content Layouts
Text and Content Layouts
Show when inserting new slides
AutoShapes
Slide 25 of 25
1_MVP Global Summit 2004

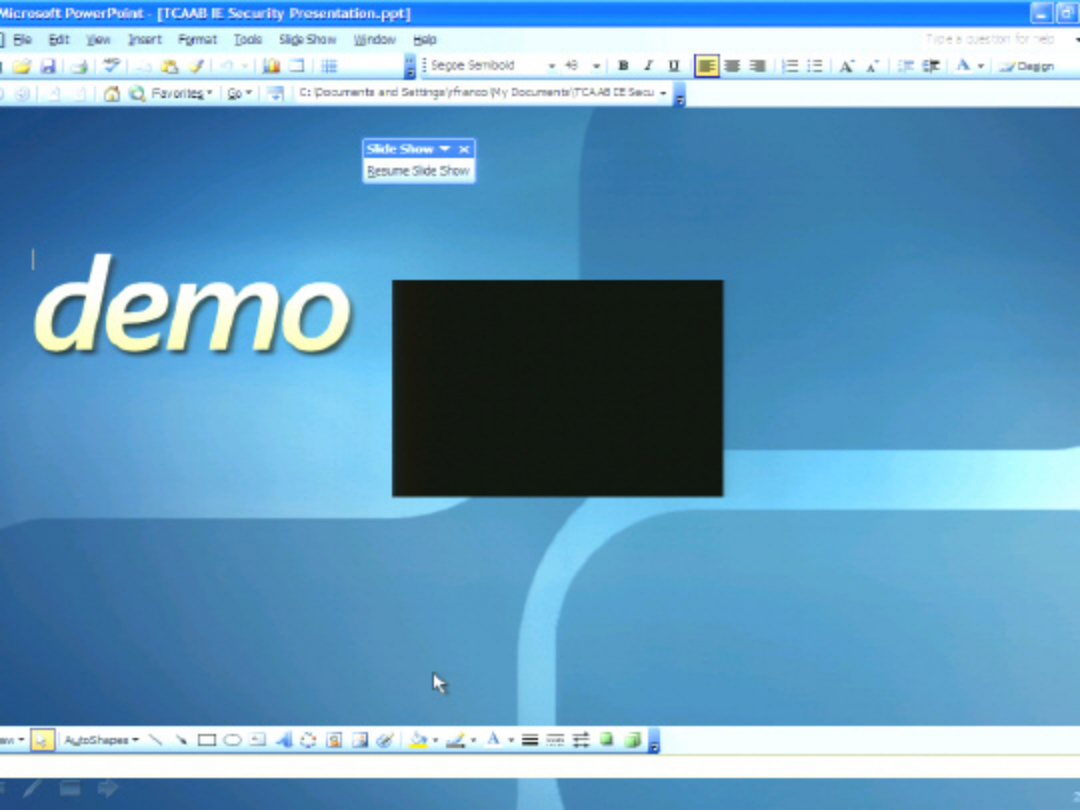
Anti-Phishing Overview

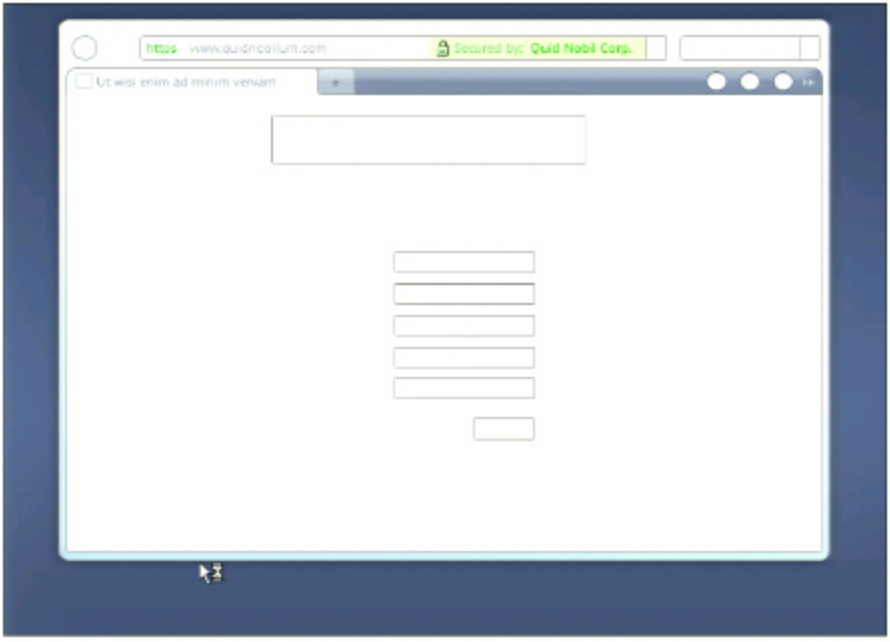
- Overview of releases to counter phishing attacks
  - MS04-004 blocked the use of the "@" sign in URLs - Spring '04
    - Eg. http://www.rbc.com@http://www.badguys.com
  - IE for XP SP2 fights phishing with pop-up blocking and improved UI – Summer '04
  - Anti-Phishing filter - Summer '05
  - IE 7 – Dec '05

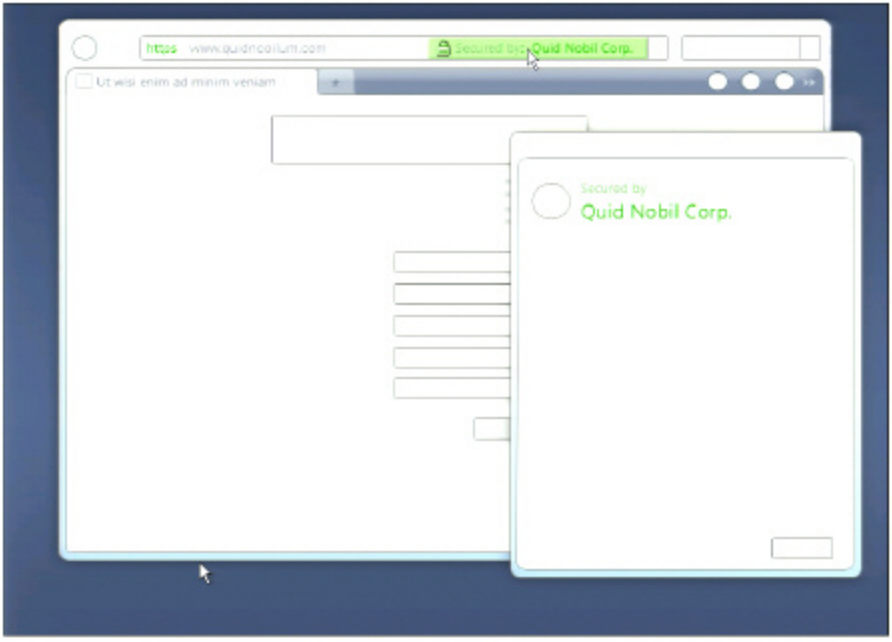
Anti-Phishing Filter Heuristics

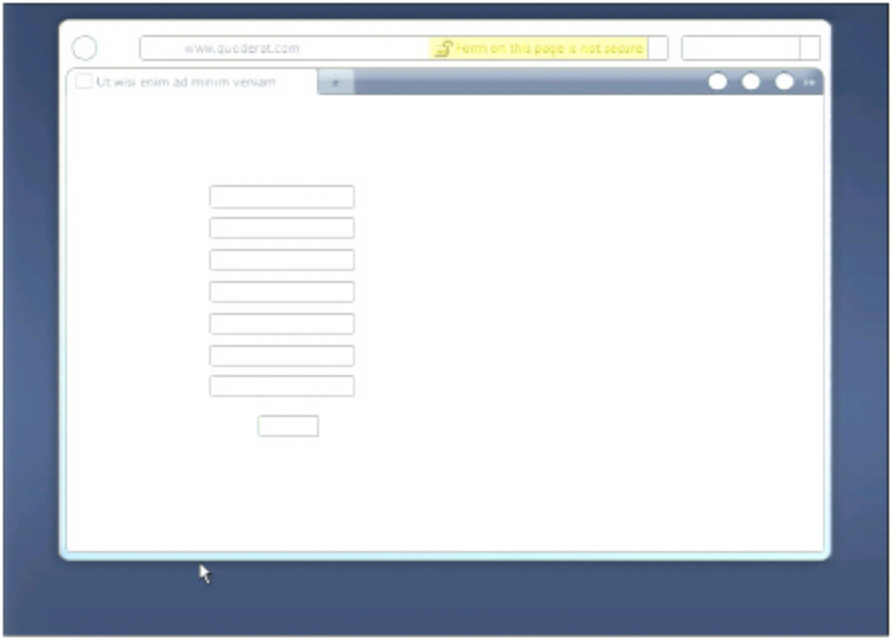
- URL Heuristics
  - URL Tricks – "@" tricks and variants, non standard ports
  - Use of IP Addresses
  - URL Obfuscation – Excessive escaping
  - Links from e-mails – web based e-mail clients
- Web Page Heuristics
  - Detection of Forms
    - Watch specifically for requests for PII/Acct Info
    - Mismatch hosted site vs. where POST goes
  - SSL enabled
  - Mis-Matched Links

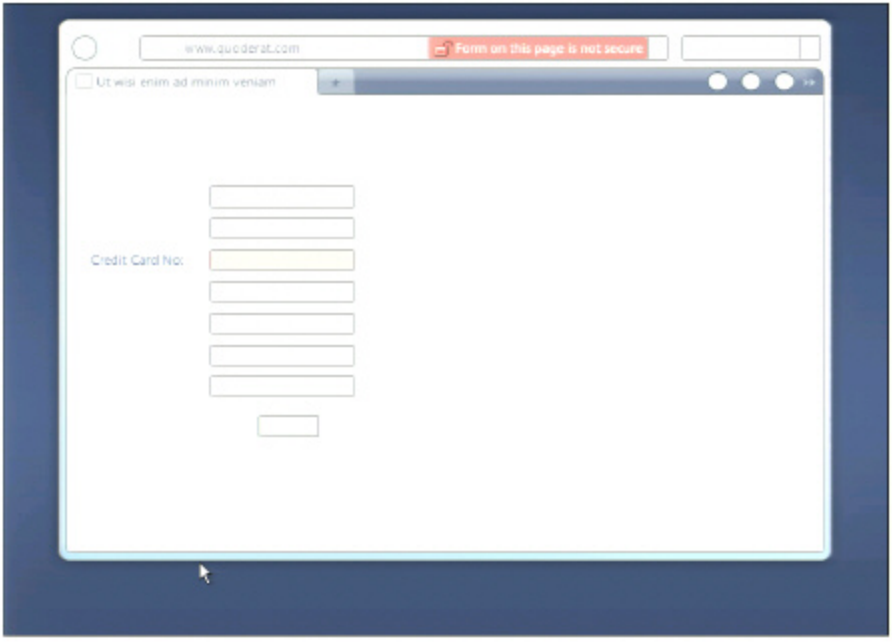
demo

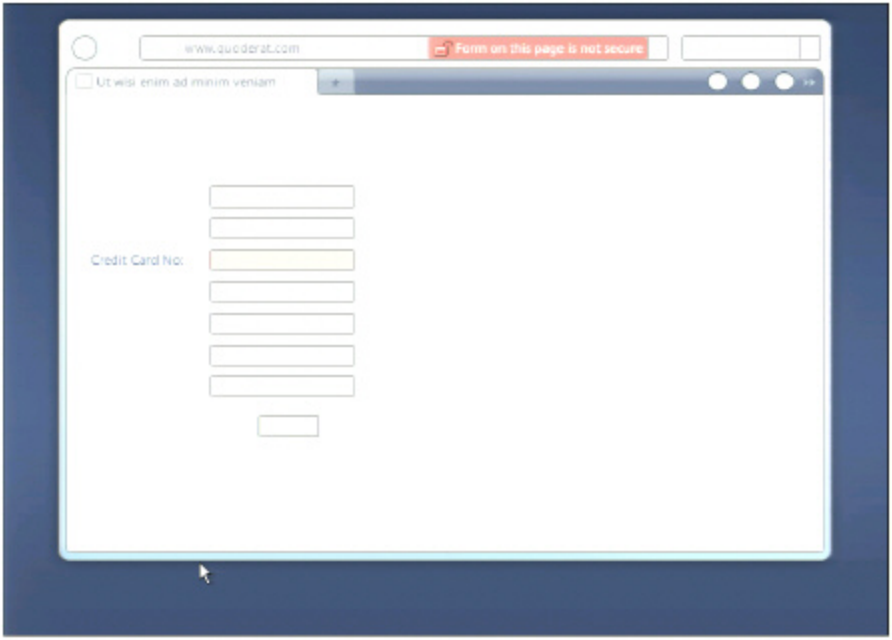

Microsoft PowerPoint - [TCAAB IE Security Presentation.ppt]
File Edit View Insert Format Tools Slide Show Window Help
Type a question for help
Segoe Semibold
Design
Favorites
Go
C:\Documents and Settings\yfranco\My Documents\TCAAB IE Secu
Slide Show
Resume Slide Show
demo
AutoShapes

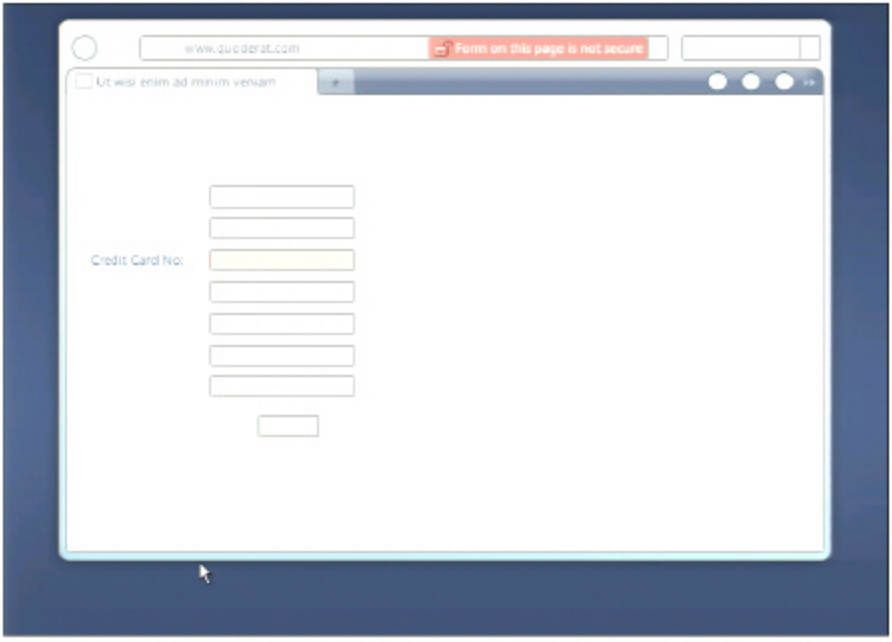

https www.quidnostrum.com
Secured by: Quid Nobil Corp.
Ut wisi enim ad minim veniam


https www.quidnobilum.com
Secured by Quid Nobil Corp.
Ut wisi enim ad minim veniam
Secured by
Quid Nobil Corp.

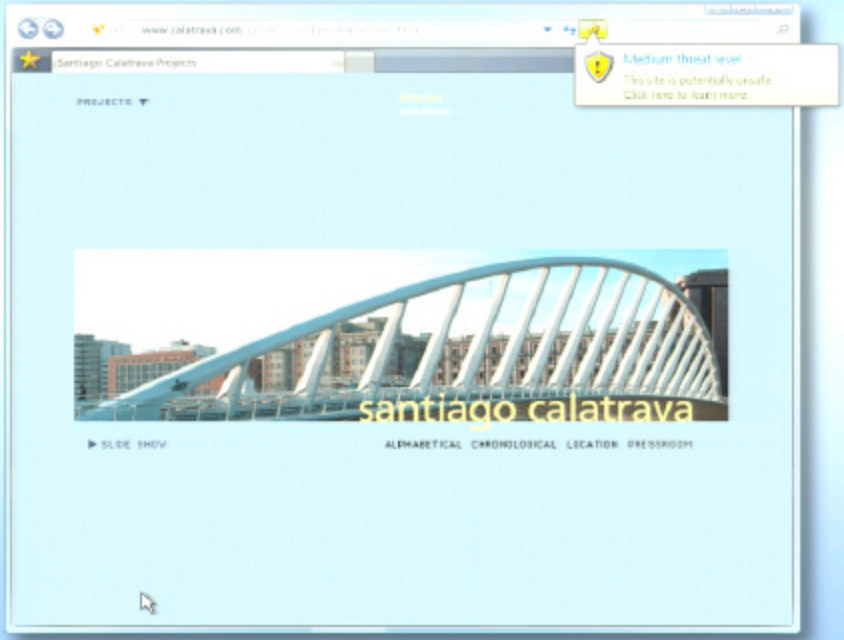

www.succerat.com
Form on this page is not secure
Ut wisi enim ad minim veniam


www.succerat.com
Form on this page is not secure
Ut wisi enim ad minim veniam
Credit Card No:


www.succerat.com
Form on this page is not secure
Ut wisi enim ad minim veniam
Credit Card No:


www.succerat.com
Form on this page is not secure
Ut wisi enim ad minim veniam
Credit Card No:

Phishing_9_dialog.jpg - Windows Picture and Fax Viewer
www.calatrava.com
Santiago Calatrava Projects
Zoom
PROJECTS
Anti Phishing Warning
This site is a confirmed phishing site. It's not safe to continu browsing this site.
Learn more about phishing threats
Block Site
Continu Anyway
santiago calatrava
SLIDE SHOW
ALPHABETICAL CHRONOLOGICAL LOCATION PRESSROOM
start


www.calatrava.com
Santiago Calatrava Projects
Medium threat level
This site is potentially unsafe.
Click here to learn more.
PROJECTS
santiago calatrava
SLIDE SHOW
ALPHABETICAL CHRONOLOGICAL LOCATION PRESSROOM